AMENDMENT TO THE CLAIMS

The following listing of claims replaces all prior versions.

1. (Currently Amended) A ~~machine implemented~~ method for securing data in communications between a client and server using an unencrypted transfer protocol that does not encrypt a payload defined by the transfer protocol, the method comprising the computer-implemented steps of:

selecting a subset of data for encryption from a set of data to be communicated between the client and the server in a particular payload of the unencrypted transfer protocol;

determining a secret integer that is unique for the subset among a plurality of subsets in a plurality of payloads, wherein the secret integer associated with the particular payload is unique relative to secret integers associated with other payloads of the plurality of payloads, wherein determining the secret integer comprises:

determining a shared secret key based on a first integer and a first public key associated with a receiving device of the client and the server; and

selecting the secret integer based on the shared secret key;

~~secret~~ encrypting the subset of data using at least the secret integer to generate encrypted data that is impractical for a device other than the client and the server to decrypt; and

sending, from a sending device of the client and the server to [[a]] the receiving device ~~of the client and the server~~, in the particular payload, the encrypted data and clue information to determine, only at the client and the server, the secret integer for decrypting the encrypted data.

2. (Original) A method as recited in Claim 1, wherein the unencrypted transfer protocol is Hypertext Transfer Protocol (HTTP).

3. (Currently Amended) A method as recited in Claim 1, said step of determining a secret integer that is unique for the subset further comprising the steps of:

generating [[a]] the first integer using a random number generator[[;]]

~~determining a shared secret key to be shared with the receiving device based on the first integer and a first public key associated with the receiving device; and~~

~~selecting the secret integer based on the shared secret key~~.

4. (Original) A method as recited in Claim 3, said step of sending the information to determine the secret integer further comprising the steps of:

determining a second public key associated with the sending device based on the first integer; and

including the second public key in the information to determine the secret integer.

5. (Original) A method as recited in Claim 3, said step of sending the information to determine the secret integer further comprising the steps of:

determining a plurality of second public keys associated with the sending device based on the first integer, wherein each of the second public keys is associated with one of a plurality of subsets from the set of data; and

including the plurality of second public keys in the information to determine the secret integer.

6. (Previously Presented) A method as recited in Claim 3, said step of selecting the secret integer further comprising the step of applying a particular hash function to the shared secret key to generate the secret integer.

7. (Original) A method as recited in Claim 3, said step of generating encrypted data further comprising the step of performing an exclusive or (XOR) operation between corresponding bits of the subset and the secret integer to generate the encrypted data.

8. (Currently Amended) A method as recited in Claim 1, wherein:

said step of determining the secret integer further comprises the step of applying a particular hash function a plurality of times to [[a]] <u>the</u> shared secret key shared with the receiving device; and

said step of sending the information to determine the secret integer further comprises the step of storing, as part of the clue information, data that indicates a number of times the particular hash function has been applied.

9. (Currently Amended) A method as recited in Claim 8, said step of determining the secret integer further comprising the steps of:

determining a [[first]] second integer formed after the particular hash function is applied the number of times indicated in the information;

determining a ~~second~~ third integer formed after the particular hash function is applied fewer times than the number of times indicated in the information; and

performing an exclusive or (XOR) operation between corresponding bits of the [[first]] second integer and the ~~second~~ third integer.

10. (Currently Amended) A method as recited in Claim 8, said step of determining the secret integer further comprising the steps of:

determining a [[first]] second integer formed after the particular hash function is applied the number of times indicated in the information;

determining a ~~second~~ third integer formed after a second hash function is applied for the number of times indicated in the information, wherein the second hash function is different from the particular hash function that is used to determine the [[first]] second integer; and

performing an exclusive or (XOR) operation between corresponding bits of the [[first]] second integer and the ~~second~~ third integer.

11. (Currently Amended) A method as recited in Claim 8, ~~further comprising, before said step of determining the secret integer, performing the steps of:~~

wherein determining the shared secret key is based on a particular communication between the client and the server; and

further comprising storing the shared secret key in a secure data structure.

12. (Original) A method as recited in Claim 1, wherein the secret integer has a particular number of bits fixed for all subsets in all payloads communicated during a communication session between the client and the server.

13. (Original) A method as recited in Claim 1, wherein the secret integer has a number of bits that varies in accordance with lengths of payloads that are communicated during a communication session between the client and the server.

14 – 23. (Canceled)

24. (Currently Amended) A computer-readable medium carrying one or more sequences of instructions for securing data in communications between a client and server using an unencrypted transfer protocol that does not encrypt a payload defined by the transport protocol, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

selecting a subset of data for encryption from a set of data to be communicated between the client and the server in a particular payload of the unencrypted transfer protocol;

determining a secret integer that is unique for the subset among a plurality of subsets in a plurality of payloads, wherein the secret integer associated with the particular payload is unique relative to secret integers associated with other payloads of the plurality of payloads, wherein determining the secret integer comprises:

determining a shared secret key based on a first integer and a first public key associated with a receiving device of the client and the server; and

selecting the secret integer based on the shared secret key;

encrypting the subset of data using at least the secret integer to generate encrypted data that is practically unintelligible to a device other than the client and the server; and

sending, from a sending device of the client and the server to [[a]] the receiving device ~~of the client and the server~~, in the particular payload, the encrypted data and information to determine, only at the client and the server, the secret integer for decrypting the encrypted data.

25. (Canceled)

26. (Currently Amended) An apparatus for securing data in communications between a client and server using an unencrypted transfer protocol that does not encrypt a payload defined by the transport protocol, comprising:

means for selecting a subset of data for encryption from a set of data to be communicated between the client and the server in a particular payload of the unencrypted transfer protocol;

means for determining a shared secret key based on a first integer and a first public key associated with a receiving device of the client and the server;

means for determining a secret integer that is unique for the subset among a plurality of subsets in a plurality of payloads, wherein the secret integer associated with the particular payload is unique relative to secret integers associated with other payloads of the plurality of payloads, wherein the means for determining the secret integer comprise means for selecting the secret integer based on the shared secret key;

means for encrypting the subset of data using at least the secret integer to generate, encrypted data that is practically unintelligible to a device other than the client and the server; and

means for sending to [[a]] the receiving device ~~of the client and the server~~, in the particular payload, the encrypted data and information to determine, only at the client and the server, the secret integer for decrypting the encrypted data.

27. (Canceled)

28. (Currently Amended) An apparatus for securing data in communications between a client and server using an unencrypted transfer protocol that does not encrypt a payload defined by the transport protocol, comprising:

a network interface that is coupled to the data network for sending one or more packet flows thereto;

a processor;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

selecting a subset of data for encryption from a set of data to be communicated between the client and the server in a particular payload of the unencrypted transfer protocol;

determining a secret integer that is unique for the subset among a plurality of subsets in a plurality of payloads, wherein the secret integer associated with the particular payload is unique relative to secret integers associated with other payloads of the plurality of payloads, wherein determining the secret integer comprises:

determining a shared secret key based on a first integer and a first public key associated with a receiving device of the client and the server; and

selecting the secret integer based on the shared secret key;

encrypting the subset of data using at least the secret integer to generate encrypted data that is practically unintelligible to a device other than the client and the server; and

sending, to [[a]] the receiving device ~~of the client and the server~~, in the particular payload, the encrypted data and information to determine, only at the client and the server, the secret integer for decrypting the encrypted data.

29. (Canceled)

30. (Previously Presented) The apparatus of Claim 28, wherein the unencrypted transfer protocol is Hypertext Transfer Protocol (HTTP).

31. (Currently Amended) The apparatus of Claim 28, wherein the sequences of instructions that cause the processor to perform determining a secret integer that is unique for the subset comprise sequences of instructions which, when executed by the processor, cause the processor to perform:

generating [[a]] the first integer using a random number generator[[;]]

~~determining a shared secret key to be shared with the receiving device based on the first integer and a first public key associated with the receiving device; and~~

~~selecting the secret integer based on the shared secret key~~.

32. (Previously Presented) The apparatus of Claim 31, wherein the sequences of instructions that cause the processor to perform sending the information to determine the secret integer comprise sequences of instructions which, when executed by the processor, cause the processor to perform:

determining a second public key associated with the sending device based on the first integer; and

including the second public key in the information to determine the secret integer.

33. (Previously Presented) The apparatus of Claim 31, wherein the sequences of instructions that cause the processor to perform sending the information to determine the secret integer comprise sequences of instructions which, when executed by the processor, cause the processor to perform:

determining a plurality of second public keys associated with the sending device based on the first integer, wherein each of the second public keys is associated with one of a plurality of subsets from the set of data; and

including the plurality of second public keys in the information to determine the secret integer.

34. (Previously Presented) The apparatus of Claim 31, wherein the sequences of instructions that cause the processor to perform selecting the secret integer comprise sequences of instructions which, when executed by the processor, cause the processor to perform applying a particular hash function to the shared secret key to generate the secret integer.

35. (Previously Presented) The apparatus of Claim 31, wherein the sequences of instructions that cause the processor to perform generating encrypted data comprise sequences of instructions which, when executed by the processor, cause the processor to perform an exclusive or (XOR) operation between corresponding bits of the subset and the secret integer to generate the encrypted data.

36. (Currently Amended) The apparatus of Claim 28, wherein the sequences of instructions that cause the processor to perform determining the secret integer comprise sequences of instructions which, when executed by the processor, cause the processor to perform applying a particular hash function a plurality of times to [[a]] the shared secret key shared with the receiving device; and

wherein the sequences of instructions that cause the processor to perform sending the information to determine the secret integer comprise sequences of instructions which, when executed by the processor, cause the processor to perform storing, as part of the clue information, data that indicates a number of times the particular hash function has been applied.

37. (Currently Amended) The apparatus of Claim 36, wherein the sequences of instructions that cause the processor to perform determining the secret integer comprise sequences of instructions which, when executed by the processor, cause the processor to perform:

determining a [[first]] second integer formed after the particular hash function is applied the number of times indicated in the information;

determining a ~~second~~ third integer formed after the particular hash function is applied fewer times than the number of times indicated in the information; and

performing an exclusive or (XOR) operation between corresponding bits of the [[first]] second integer and the ~~second~~ third integer.

38. (Currently Amended) The apparatus of Claim 36, wherein the sequences of instructions that cause the processor to perform determining the secret integer comprise sequences of instructions which, when executed by the processor, cause the processor to perform:

determining a [[first]] second integer formed after the particular hash function is applied the number of times indicated in the information;

determining a ~~second~~ third integer formed after a second hash function is applied for the number of times indicated in the information, wherein the second hash function is different from the particular hash function that is used to determine the [[first]] second integer; and

performing an exclusive or (XOR) operation between corresponding bits of the [[first]] second integer and the ~~second~~ third integer.

39. (Currently Amended) The apparatus of Claim 36, wherein the sequences of instructions that cause the processor to perform determining the shared secret key comprise sequences of instructions which, when executed by the processor, cause the processor to perform:

determining the shared secret key based on a particular communication between the client and the server; and

further comprising sequences of instructions which, when executed by the processor, cause the processor to perform the steps of:

~~before said step of determining the secret integer:~~

~~determining the shared secret key based on a particular communication between the client and the server; and~~

storing the shared secret key in a secure data structure.

40. (Previously Presented) The apparatus of Claim 28, wherein the secret integer has a particular number of bits fixed for all subsets in all payloads communicated during a communication session between the client and the server.

41. (Previously Presented) The apparatus of Claim 28, wherein the secret integer has a number of bits that varies in accordance with lengths of payloads that are communicated during a communication session between the client and the server.

42. (Previously Presented) The apparatus of Claim 26, wherein the unencrypted transfer protocol is Hypertext Transfer Protocol (HTTP).

43. (Currently Amended) The apparatus of Claim 26, wherein the means for determining

a generating [[a]] the first integer using a random number generator[[;]]

~~determining a shared secret key to be shared with the receiving device based on the first integer and a first public key associated with the receiving device; and~~

~~selecting the secret integer based on the shared secret key~~.

44. (Previously Presented) The apparatus of Claim 43, wherein the means for sending the information to determine the secret integer comprises means for:

determining a second public key associated with the sending device based on the first integer; and

including the second public key in the information to determine the secret integer.

45. (Previously Presented) The apparatus of Claim 43, wherein the means for sending the information to determine the secret integer comprises means for:

determining a plurality of second public keys associated with the sending device based on the first integer, wherein each of the second public keys is associated with one of a plurality of subsets from the set of data; and

including the plurality of second public keys in the information to determine the secret integer.

46. (Previously Presented) The apparatus of Claim 43, wherein the means for selecting the secret integer comprises means for applying a particular hash function to the shared secret key to generate the secret integer.

47. (Previously Presented) The apparatus of Claim 43, wherein the means for generating encrypted data comprises means for performing an exclusive or (XOR) operation between corresponding bits of the subset and the secret integer to generate the encrypted data.

48. (Currently Amended) The apparatus of Claim 26, wherein the means for determining the secret integer comprises means for applying a particular hash function a plurality of times to [[a]] the shared secret key shared with the receiving device; and

wherein the means for sending the information to determine the secret integer comprise comprises means for storing, as part of the clue information, data that indicates a number of times the particular hash function has been applied.

49. (Currently Amended) The apparatus of Claim 48, wherein the means for determining the secret integer comprises means for:

determining a [[first]] second integer formed after the particular hash function is applied the number of times indicated in the information;

determining a ~~second~~ third integer formed after the particular hash function is applied fewer times than the number of times indicated in the information; and

performing an exclusive or (XOR) operation between corresponding bits of the [[first]] second integer and the ~~second~~ third integer.

50. (Currently Amended) The apparatus of Claim 48, wherein the means for determining the secret integer comprises means for:

determining a [[first]] second integer formed after the particular hash function is applied the number of times indicated in the information;

determining a ~~second~~ third integer formed after a second hash function is applied for the number of times indicated in the information, wherein the second hash function is different from the particular hash function that is used to determine the [[first]] second integer; and

performing an exclusive or (XOR) operation between corresponding bits of the [[first]] second integer and the ~~second~~ third integer.

51. (Currently Amended) The apparatus of Claim 48, further comprising means for:

determining~~, before said step of determining the secret integer,~~ the shared secret key based on a particular communication between the client and the server; and

storing~~, before said step of determining the secret integer,~~ the shared secret key in a secure data structure.

52. (Previously Presented) The apparatus of Claim 26, wherein the secret integer has a particular number of bits fixed for all subsets in all payloads communicated during a communication session between the client and the server.

53. (Previously Presented) The apparatus of Claim 26, wherein the secret integer has a number of bits that varies in accordance with lengths of payloads that are communicated during a communication session between the client and the server.